COMOMAGINST 2280.1C
N6
27 May 03

COMOMAG INSTRUCTION 2280.1C

Subj: SECURE TELEPHONE UNIT (STU) III MANAGEMENT PROCEDURES

Ref: (a) Secure Telephone Unit Third Generation (STU-III)
COMSEC Material Management Manual, CMS 6
(b) Type 2 STU-III Key Management Plan, EKMS-702.02

Encl: (1) Sample STU-III Standard Operating Procedures

1. Purpose. To establish guidelines for the control, use and accountability of STU-III terminals and cryptographic ignition keys for COMOMAG staff personnel.

2. Cancellation. COMOMAG/MOMAGINST 2280.1B. This instruction is a major revision and should be read in its entirety.

3. Discussion. The Secure Telephone Unit Third Generation (STU-III) is a low-cost, reliable and user-friendly telephone system that provides secure communications for both the U.S. government and government-sponsored user communities. The STU-III may be used as a standard telephone in a secure or non-secure mode or as a secure data transmission device. The system operates over existing U.S. commercial, Defense Switch Network (DSN) and overseas telephone networks. Within the Mobile Mine Assembly Group (MOMAG) community, STU-III secure communications are restricted to an information security classification level of Secret and below.

4. Responsibilities

a. Command Authority. A command authority is defined as an activity that has been granted an active STU-III account. Commander, Mine Warfare Command (COMINEWARCOM) (N61) will serve as the command authority for the COMOMAG Staff. Mobile Mine Assembly Units/ Detachment (MOMAUs/MOMAD) sites with active STU-III accounts are designated as command authority for their devices.

b. Local Holder. A local holder is defined as a command whose STU-III materials are issued by a local command authority. The command authority for those MOMAU/MOMAD sites identified as a local holder is the command that issued their STU-III devices. Command authority responsibilities are outlined in chapter 4 of reference (b).

c. User Representative. All activities designated as local holders will identify a user representative responsible for all STU-III materials issued by their respective command authority. Since the command authority is the designating authority for a user representative, the respective command authority must approve those individuals recommended as user representatives. The user representative’s responsibilities are outlined in chapter 4 of reference (b).

d. Custodians. The Commanding Officers/Officer-in-Charge (COs/OIC) of MOMAU/MOMAD sites with an active STU-III account must appoint a STU-III Custodian in writing. The custodian will be responsible for the proper receipt, storage, inventory, administration, destruction and/or transfer of STU-III materials issued to the account. Each account holder must allocate at least one alternate custodian who remains actively involved in the account's daily administration and can assume full responsibility for the account at any time. Allocation requirements and a sample appointment letter are contained in reference (a).

e. STU-III Key Holder. A STU-III key holder is any person signing for and assuming custody of a cryptographic ignition key. The key holder is responsible for the proper use and stowage of all assigned keys. Their responsibilities include but are not limited to:

(1) Properly safeguarding and stowing all cryptographic ignition keys in their custody.

(2) Making each cryptographic ignition key available during normal working hours.

(3) Reporting the loss, destruction, improper use and/or malfunction of cryptographic ignition keys to the custodian or user representative.

f. STU-III User. A STU-III user is any person using a STU-III telephone in a secure or non-secure mode. Each STU-III user is responsible for:

(1) Verifying information displayed in the information window while in the secure mode. When a discrepancy occurs, i.e., the activity displayed in the information window is different than that of the party called, the discrepancy will be reported to the remote party and to the custodian or user representative.

(2) Ensuring conversations are limited to the classification level for which both the sending and receiving parties are cleared.

(3) Ensuring classified information is not transmitted or discussed on a terminal with a failed window display.

g. Maintenance and Repair. STU-III terminals requiring repair must be handled in accordance with reference (a). If a terminal or cryptographic ignition key is not functioning correctly; the responsible key holder will contact the STU-III Custodian or user representative for corrective action. If the device is determined to be defective, the command authority or user representative will:

(1) Contact the office of the Director, Communications Security Management System (DCSMS) for disposition instructions. The telephone number is DSN 764-0311/0250 or commercial (202) 764-0311/0250.

(2) If the device must be returned to the Crypto Repair Facility, the device will be packaged and mailed to VAE Systems ATTN: CMS Custodian, 821 Live Dr, Chesapeake, VA 23320-2601.

h. Operating Procedures. To prevent inadvertent erasure of cryptographic ignition keys and/or terminal configurations, the custodian or user representative must be present when STU-III terminals are disconnected, moved or reconfigured.

i. MOMAU/MOMAD sites will publish standard operating procedures for all terminals in their custody. Enclosure (1) can be used as a sample SOP.

/s/
T. W. AUBERRY

Distribution:
COMOMAGINST 5216.1T
List I
List II (Case A, Case B (COMINEWARCOM only))
List III

SAMPLE STU-III STANDARD OPERATING PROCEDURES

1. To make a non-secure call from a STU-III terminal, the following procedures should be followed:

a. First dial 9 to obtain a dial tone.

b. If calling on-base, dial 1 + the four-digit extension

c. If calling off-base, dial 9 + the local seven digit number

d. If calling DSN in-CONUS, dial 8 + the seven digit number

e. If calling DSN overseas, dial 8 + (314 for the European AOR)/ (315 for Pacific AOR) + the seven digit number.

f. If calling commercial long distance, dial 1 + the area code + the seven digit number.

2. To make a secure call from a STU-III terminal, the following procedures should be followed:

a. Retrieve the terminal's cryptographic ignition key.

NOTE: Cryptographic ignition keys may remain inserted in their respective terminals during the work day. After working hours, they must be in the key holder's personal possession or locked in a security container.

b. Insert the cryptographic ignition key and turn clockwise.

c. Place a non-secure call as described in the non-secure procedures.

d. Notify the remote party that the conversation will be classified and the level of classification. Ensure the party is cleared for the appropriate level.

e. Press the "secure voice" button. The "secure voice" light will blink and the display will indicate that the STU-III is going secure. Once secure mode is established, the "secure voice" light will remain constant and the "non-secure" or "voice" light will be extinguished. Ensure the remote activity's identification and the security level on the display are accurate. If the secure mode is not established or the display indicates that the key has expired, report the discrepancy to the remote party and contact the STU-III Custodian.

f. Press the "non-secure" or "voice" key to return to the non-secure mode or replace the handset to end the call.